

02-01-06

ATTORNEY DOCKET NO.
062891.0673

PATENT APPLICATION
USSN 10/072,069

AF \$
[Signature]

1



**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
ON APPEAL FROM THE EXAMINER TO THE BOARD
OF PATENT APPEALS AND INTERFERENCES**

In re Application of: McDaniel, David W.
Serial No.: 10/072,069
Filing Date: February 05, 2002
Confirmation No. 1183
Group Art Unit: 2154
Examiner: Ashokkumar B. Patel
Title: ADDRESS HOPPING OF PACKET-BASED
 COMMUNICATIONS

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

APPEAL BRIEF

Appellant has appealed to this Board from the decision of the Examiner, contained in a Final Office Action mailed July 26, 2005 ("*Final Office Action*") and the Advisory Action mailed November 10, 2005 ("*Advisory Action*"), finally rejecting Claims 1-27. Appellant mailed a Notice of Appeal on November 28, 2005. Appellant respectfully submits this Appeal Brief for consideration of the Board.

02/02/2006 DEMMANU1 00000046 10072069

01 FC:1402

500.00 OP

Table Of Contents

Real Party In Interest	4
Related Appeals And Interferences	5
Status Of Claims	6
Status of Amendments	7
Summary of Claimed Subject Matter	8
Grounds Of Rejection To Be Reviewed On Appeal	10
I. Whether Claims 1-3, 5, 7, 14, 15, 18, 20, 21, 24, and 26 are anticipated under 35 U.S.C. § 102(b) by PCT Application WO0070458 to <i>Sheymov</i> , et al. (" <i>Sheymov</i> ")	10
II. Whether Claims 10-13 are anticipated under 35 U.S.C. § 102(e) by U.S. Published Application No. 2004/0003116 to <i>Munger</i> , et al. (" <i>Munger</i> ").	10
III. Whether Claims 4, 6, 9, 16, 17, 19, 22, 23, 25, and 27 are obvious under 35 U.S.C. § 103(a) in view of the proposed combination of <i>Sheymov</i> with <i>Munger</i>	10
IV. Whether Claim 8 is obvious under 35 U.S.C. § 103(a) in view of the proposed combination of <i>Sheymov</i> with U.S. Published Application No. 2002/10091941 to <i>Challenger</i> , et al. (" <i>Challenger</i> ").	10
Argument	11
I. <i>Sheymov</i> fails to describe, expressly or inherently, at least three elements required by Claims 1-3, 5, 7, 14, 15, 18, 20, 21, 24, and 26.	11
A. <i>Sheymov</i> does not teach that the address modification process is performed independently from both the first user interface device and the second user interface device.	12
B. <i>Sheymov</i> does not teach receiving at a first translation module a stream comprising a plurality of packets, where each packet has an original destination address.	15
C. <i>Sheymov</i> does not teach that the modified destination addresses are resolvable by the second translation module to the original destination address.	16
II. <i>Munger</i> fails to describe a method comprising negotiating translation parameters comprising an original destination address and changing the packet to have the original destination address as recited in Claims 10-13.	17
III. The proposed <i>Sheymov-Munger</i> combination fails to teach or suggest all limitations of Claims 4, 6, 9, 16, 17, 19, 22, 23, 25, and 27	19

A.	<i>Sheymov</i> and <i>Munger</i> , whether taken alone or in combination, fail to teach or suggest all limitations of dependent Claims 4, 6, 9, 16, 17, 19, 22, 23, and 25 and independent Claim 27.	19
B.	There is no suggestion or motivation in the cited references or in the prior art to combine <i>Sheymov</i> and <i>Munger</i>	21
IV.	The proposed <i>Sheymov-Challenger</i> combination fails to teach or suggest all limitations of Claim 8.	22
	Conclusion	24
	Appendix A: Claims Involved In Appeal	25
	Appendix B: Evidence	33
	Appendix C: Related Proceedings	34

Real Party In Interest

The real party in interest for this Application under appeal is Cisco Technology, Inc.
of San Jose, California.

Related Appeals And Interferences

The Appellant, the undersigned Attorney for Appellant, and the Assignee know of no applications on appeal that may directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

Status Of Claims

Claims 1-27 were rejected by the *Final Office Action*. Appellant presents all pending claims for appeal – Claims 1-27 – and sets forth these claims in Appendix A.

Status of Amendments

The claims on appeal and which appear in Appendix A of this Appeal Brief represent the form of the claims as of the time of the *Final Office Action* dated July 26, 2005. Appellant filed no amendments to the claims after the *Final Office Action*.

Summary of Claimed Subject Matter

The claims of the present application are directed to methods for securing packet-based communications and associated components used to implement the methods. A first user interface device (14, 26) sends a communication to a second user interface device (14, 26). Specification, Figure 1. These communications either begin as packet-based communications or are converted by other elements into packet-based communications. *Id.* at page 6, lines 5-15. In order to increase security of these transmissions, translation modules (12) use address hopping to obscure source and/or destination addresses of packets. *Id.* at Figure 1; page 6, lines 12-15; page 7, line 26 - page 8, line 4.

Using address hopping, translation modules modify the source and/or destination address of a packet. *Id.* at page 8, lines 26-29. Translation modules modify the addresses to values that may be resolved by a remote translation module to the original source and destination addresses of the packet. *Id.* For example, a first translation module receives a packet from a first user interface device. The first translation module may modify the source and destination address of the packet and forward it to the second translation module. After receiving the modified packet, the second translation module can determine the original source and destination addresses from the modified packet. Thus, the second translation module can convert the modified source and destination address into the original source and destination addresses. *Id.* at page 8, line 29 - page 9, line 6.

In a stream of packets, translation modules can secure some or all of the packets using address hopping. *Id.* at page 8, lines 25-26. Additionally, the packets in the stream may be given different source and/or destination addresses. *Id.* page 9, lines 11-21. For example, each consecutive packet may be modified differently by the translation module. *Id.* at page 9, lines 19-21. Thus, potential eavesdroppers are unable to focus on any particular address, severely limiting a third party's ability to intercept and interpret communications. *Id.* page 3, lines 20-22; page 9, lines 11-13. In the claims, this address modification process is preformed independently from both the first user interface device and the second user interface device.

The following discussion identifies the claimed means plus function limitations and, for each such limitation, provides example structures and discussion in the specification for performing the recited functions:

1. means for receiving at the first translation module a stream comprising a plurality of packets

Example structures for performing the recited function include translation modules 12, including external interface 52, internal interface 52 and controller 50, call agent 22, and media gateways 24, as described in the specification at 6:2-15, 6:30-7:16, 7:26-8:4, 8:25-11:8, 11:15-28, 12:14-14:3, 14:4-9, 16:1-2.

2. means for performing at the first translation module an address modification process

Example structures for performing the recited function include translation modules 12, including controller 50, as described in the specification at 6:12-15, 7:26-8:4, 8:25-11:8, 11:24-28, 12:14-14:3, 14:27-15:2, 16:4-6.

Grounds Of Rejection To Be Reviewed On Appeal

Appellant requests that the Board review:

- I. Whether Claims 1-3, 5, 7, 14, 15, 18, 20, 21, 24, and 26 are anticipated under 35 U.S.C. § 102(b) by PCT Application WO0070458 to *Sheymov*, et al. ("*Sheymov*").
- II. Whether Claims 10-13 are anticipated under 35 U.S.C. § 102(e) by U.S. Published Application No. 2004/0003116 to *Munger*, et al. ("*Munger*").
- III. Whether Claims 4, 6, 9, 16, 17, 19, 22, 23, 25, and 27 are obvious under 35 U.S.C. § 103(a) in view of the proposed combination of *Sheymov* with *Munger*.
- IV. Whether Claim 8 is obvious under 35 U.S.C. § 103(a) in view of the proposed combination of *Sheymov* with U.S. Published Application No. 2002/10091941 to *Challenger*, et al. ("*Challenger*").

Argument

I. *Sheymov* fails to describe, expressly or inherently, at least three elements required by Claims 1-3, 5, 7, 14, 15, 18, 20, 21, 24, and 26.

Consider Appellant's independent Claim 1, which recites:

A method for securing packet-based communications comprising:
receiving at a first translation module a stream comprising a plurality of packets regarding a communication from a first user interface device intended for a second user interface device, each packet having an original destination address and an original source address; and
for each of the packets, performing an address modification process including changing the original destination address to a selected one of a plurality of modified destination addresses assigned to a second translation module remote from the first translation module, wherein each of the selected modified destination addresses is resolvable by the second translation module to the original destination address for forwarding the packet to the second user interface device;
wherein the address modification process is performed independently from both the first user interface device and the second user interface device.

Appellant respectfully submits that *Sheymov* fails to describe, expressly or inherently, every element of this claim, and therefore the Examiner's § 102 rejection based on *Sheymov* must fail. *See Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 U.S.P.Q.2d 1051, 1053 (Fed. Cir. 1987) (stating that a single prior art reference must describe, either expressly or inherently, each and every element of the claim in order to anticipate a claim under 35 U.S.C. § 102).

Among other elements, *Sheymov* fails to disclose that: (1) the address modification process is performed independently from both the first user interface device and the second user interface device, (2) the method comprises receiving at a first translation module a stream comprising a plurality of packets, where each packet has an original destination address, and (3) the modified destination addresses are resolvable by the second translation module to the original destination address.

In general, *Sheymov* teaches a communication network intrusion protection system in which the cyber coordinate (*i.e.*, the cyber address) of a target computer continuously changes over time, requiring a potential intruder to repeatedly guess the current location of the target computer. (*Sheymov*, pg. 4, ll. 9-16). *Sheymov* discloses a management unit that

maintains a series of tables containing the cyber addresses of the target computer. (*Id.* at ll. 16-20). The management unit distributes the cyber addresses to authorized parties, such as a user computer (distinct from the target computer). (*Id.*). At the user computer, a computer address book stores the received variable cyber addresses for the target computer along with an alphabetic destination address. (*Id.* at pg. 7, ll. 20-22). The alphabetic destination address is presented to an actual user of the user computer to identify the target computer, but this address is not used for actually addressing any communication. (*Id.* at pg. 7, ll. 18-24). When a user wants to transmit information to the target computer, the user selects the alphabetic address, and the user computer automatically substitutes the current cyber address of the target computer in packets sent to the target computer. (*Id.* at pg. 6, ll. 23-31; pg. 7, ll. 22-24).

A. *Sheymov* does not teach that the address modification process is performed independently from both the first user interface device and the second user interface device.

Claim 1 requires a method “wherein the address modification process is performed independently from both the first user interface device and the second user interface device.” For each packet in a received stream of packets, the address modification process includes “changing the original destination address [in each received packet] to a selected one of a plurality of modified destination addresses.” (Claim 1). *Sheymov* fails to disclose these claimed aspects.

As teaching these aspects, the *Final Office Action* cites to page 7, lines 16-18 and 20-24 in *Sheymov*. (*Final Office Action*, pg. 2, 4; *see also Advisory Action*, pg. 2). These portions of *Sheymov* recite:

A management system 18 periodically changes the address for the computer 14 by providing a new address from a cyber address book 20 which stores a plurality of cyber addresses. Each new cyber address is provided by the management system 18 to the router 16 and to a user computer address book 22. . . . The address book 22 contains both the alphabetic destination address for the computer 14 which is available to the user and the variable numeric cyber address which is not available to the user. When the user wants to transmit a packet of information with the alphabetic address for the computer 14, this alphabetic address is automatically substituted for the current numerical cyber address and used in the packet.

(*Sheymov*, pg. 7, lines 16-18 & 20-24). The Examiner, thus, apparently asserts that the address modification process is performed by one of the following: (1) the management system (Figure 1, item 18), (2) the router (Figure 1, item 16), or (3) the address book (Figure 1, item 22).

1. The management system 18 and the router 16 do not perform an address modification process as required by Claim 1.

A user's computer contains an address book that correlates a permanent alphabetic address with a variable cyber address. (*Sheymov*, pg. 6, ll. 25-28). The "actual communication functions are performed by the computer using the variable side of the 'address book' periodically updated by the [management system 18]." (*Id.* at pg. 14, ll. 17-19). Thus, when a user wants to transmit a packet to the permanent alphabetic address for a remote computer, the user's computer 12 automatically substitutes the corresponding variable cyber address from the address book 22. (*Id.* at pg. 7, ll. 22-24). Management unit 18 merely updates the cyber addresses contained in the user's computer address book 22.

However, appellant's Claim 1 also specifies that, for each packet in a received stream of packets, the address modification process includes "changing the original destination address to a selected one of a plurality of modified destination addresses." (emphasis added). Neither the management system 18 nor the router 16 changes the original destination address to a modified destination address for each of a plurality of packets. Accordingly, neither the management system 18 nor the router 16 performs an address modification process as required by the claims.

2. The address book 22 is associated with the user's computer and does not perform an address modification process remotely. Cyber address book 20 fails to perform an address modification process.

The Examiner also seems to assert that the address book (Figure 1, item 22) in *Sheymov* discloses "[performing] the address modification process [] independently from both the first user interface device and the second user interface device." The *Advisory Action* states:

Please refer to Fig. 1 and page 7, line 20-24 . . . "Each new cyber address is provided by the management system 18 to the router 16 and to a user computer address book 22. The address book [22] contains both the alphabetic destination address for the computer 14 . . . and the variable

numeric cyber address . . . When the user wants to transmit a packet of information with the alphabetic address for the computer 14, this alphabetic address is automatically substituted for the current numerical cyber address and used in the packet.”

Please note that Address book is associated with protected computer 14 and not the remote user’s computer 12.

(*Advisory Action*, pages 2-3; see *Sheymov* Figure 1 and pg. 7, ll. 20-24).

In *Sheymov*, a user’s computer addresses packets using cyber addresses contained in its user computer address book. If for argument’s sake this is considered an address modification, this process is not “performed independently from both the first user interface device and the second user interface device,” as required by Claim 1. As can easily be seen in Figure 1 of *Sheymov*, the address book shown by item 22 is “a user computer address book 22.” (*Sheymov*, Figure 1 and pg. 7, ll. 19-20). Thus, the address book 22 is associated with remote user 12 and not with protected computer 14, the opposite of what the Examiner asserted. (See *Advisory Action*, pg. 3). Accordingly, the user computer address book 22 fails to perform an address modification process “independently from both the first user interface device and the second user interface device.”

Appellant respectfully submits that the Examiner seems to be improperly mixing the functions and locations of user computer address book 22 and cyber address book 20, which is a separate element associated with management unit 18 and protected computer 14. Appellant agrees that the cyber address book 20 seems to be “associated with protected computer 14 and not the remote user’s computer 12.” (*Advisory Action*, pg. 3). However, cyber address book 20 fails to perform the address modification process required by Claim 1. Appellant’s Claim 1 specifies that, for each packet in a received stream of packets, the address modification process includes “changing the original destination address to a selected one of a plurality of modified destination addresses.” Cyber address book 20 fails to change the original destination address to a modified destination address for each of the packets, as required by the claims. Accordingly, the cyber address book 20 fails to perform an address modification process as required by the claims.

Accordingly, *Sheymov* does not describe, expressly or inherently, a method “wherein the address modification process is performed independently from both the first user interface device and the second user interface device,” as required by Claim 1. Independent Claims 14, 20, and 26 include limitations that, for substantially similar reasons, are not taught

by *Sheymov*. Because *Sheymov* does not disclose, expressly or inherently, every element of independent Claims 1, 14, 20, and 26 and their respective dependent claims, Appellant respectfully requests the Board to reverse the Examiner's rejection of Claims 1-3, 5, 7, 14, 15, 18, 20, 21, 24, and 26 and direct the Examiner to issue a notice of allowance.

B. *Sheymov* does not teach receiving at a first translation module a stream comprising a plurality of packets, where each packet has an original destination address.

Claim 1 further requires "receiving at a first translation module a stream comprising a plurality of packets . . . , each packet having an original destination address." *Sheymov* does not disclose these claimed aspects

As teaching the original destination address, the *Final Office Action* points to the alphabetic destination address disclosed in *Sheymov*, page 7, lines 20-24. (*Final Office Action*, pg. 4). Appellant respectfully submits that *Sheymov*'s alphabetic destination address is never a part of any packet. *Sheymov* states that a user only deals with a computer's permanent identifier: the alphabetic address. (*Sheymov*, pg. 6, ll. 16-21). The user's computer contains an address book that stores both the alphabetic address and corresponding variable addresses of a target computer. (*Id.* at ll. 24-28). "While a user is working with other members of the network on the name or alphabetic address basis, the computer conducts communications based on the corresponding variable numeric or other addresses assigned for that particular time." (*Id.* at ll. 28-31). Appellant's Claim 1 specifies that "each packet [has] an original destination address" and "the original destination address [is changed] to a selected one of a plurality of modified destination addresses," with this modification process taking place independently of the user interface devices. (emphasis added).

Appellant submits that, rather than including the alphabetic destination address as part of a packet, *Sheymov*'s alphabetic destination address is substituted with the current numerical cyber address and the latter is included in packets. *Sheymov* fails to disclose that the alphabetic destination address is ever part of a packet. Rather, *Sheymov*'s cyber address is the only address used in a packet.

Thus, *Sheymov* does not describe, expressly or inherently, "receiving at a first translation module a stream comprising a plurality of packets . . . , each packet having an

original destination address,” as required by Claim 1. Independent Claims 14, 20, and 26 include limitations that, for substantially similar reasons, are not taught by *Sheymov*. Because *Sheymov* does not disclose, expressly or inherently, every element of independent Claims 1, 14, 20, and 26 and their respective dependent claims, Appellant respectfully requests the Board to reverse the Examiner’s rejection of Claims 1-3, 5, 7, 14, 15, 18, 20, 21, 24, and 26 and direct the Examiner to issue a notice of allowance.

C. *Sheymov* does not teach that the modified destination addresses are resolvable by the second translation module to the original destination address.

Claim 1 further requires that “each of the selected modified destination addresses is resolvable by the second translation module to the original destination address for forwarding the packet to the second user interface device.” *Sheymov* fails to disclose these claimed aspects.

For these aspects, the *Final Office Action* points to *Sheymov*, page 7, lines 25-28. (*Final Office Action*, pg. 5). This portion of *Sheymov* recites:

With the reference to Figures 1 and 2, when a packet is received by the gateway router or bridge 16 as indicated at 24, the cyber address is checked by the gateway router or bridge at 26, and if the destination address is correct, the packet is passed at 28 to the computer 14.

(*Sheymov*, pg. 7, ll. 25-28). However, checking for a correct address does not disclose that “each of the selected modified destination addresses is resolvable by the second translation module to the original destination address for forwarding the packet to the second user interface device.” Appellant respectfully submits that *Sheymov* provides no indication that the “selected modified destination addresses [are] resolvable by the second translation module to the original destination address,” as required by Claim 1. Moreover, if the alphabetic address is the original destination address, as the Examiner apparently asserts, *Sheymov* provides no mechanism for any devices (other than the sending computer) to resolve any addresses to the alphabetic address.

Thus, *Sheymov* does not describe, expressly or inherently, that “each of the selected modified destination addresses is resolvable by the second translation module to the original destination address for forwarding the packet to the second user interface device,” as required

by Claim 1. Independent Claims 14, 20, and 26 include limitations that, for substantially similar reasons, are not taught by *Sheymov*. Because *Sheymov* does not disclose, expressly or inherently, every element of independent Claims 1, 14, 20, and 26 and their respective dependent claims, Appellant respectfully requests the Board to reverse the Examiner's rejection of Claims 1-3, 5, 7, 14, 15, 18, 20, 21, 24, and 26 and direct the Examiner to issue a notice of allowance.

II. *Munger* fails to describe a method comprising negotiating translation parameters comprising an original destination address and changing the packet to have the original destination address as recited in Claims 10-13.

Consider Appellant's independent Claim 10, which recites:

A method for securing packet-based communications comprising:
negotiating translation parameters with a remote device for a communication stream between a first user interface device and a second user interface device, the translation parameters comprising an original destination address, a plurality of available destination addresses, and an algorithm;
determining a modified destination address from among the available destination addresses according to the algorithm;
receiving a packet of the communication stream having the modified destination address; and
changing the packet to have the original destination address, wherein the address change is performed independently from both the first user interface device and the second user interface device.

Appellant submits that *Munger* fails to describe, expressly or inherently, all elements of this claim, and therefore the Examiner's § 102 rejection based on *Munger* must fail. *See In re Robertson*, 169 F.3d 743, 745, 49 U.S.P.Q.2d 1949, 1950 (Fed. Cir. 1999) (stating that a single prior art reference must describe, either expressly or inherently, each and every element of the claim to anticipate a claim under 35 U.S.C. § 102(e)).

In general, *Munger* teaches a secure mechanism for communicating over the internet that sends packets having two-layer encryption through TARP (Tunneled Agile Routing Protocol) routers. (*Munger* at ¶ 0009). The packets exchanged between TARP terminals are encrypted packets whose true destination address is hidden. (*Id.*) Instead of indicating the final destination of the packet, the visible IP address header only specifies the next-hop in a series of TARP router hops. (*Id.*)

Among other aspects, *Munger* fails to teach a method comprising “negotiating translation parameters . . . comprising an original destination address . . .” and “changing the packet to have the original destination address,” as required by Claim 10. As teaching these claimed aspects, the *Final Office Action* points to *Munger*, paragraphs 0109, 0112, and 0117, and the *Advisory Action* further points to paragraphs 0108 and 0111 of *Munger*. (*Final Office Action*, pg. 6-7; *Advisory Action*, pg. 5).

In *Munger*, to establish a secure session with a router, a client computer sends a request that includes the client’s current IP address and a known IP address for the router. (*Munger*, ¶ 0112). The router responds by sending “the transmit and receive hopblocks that the client 801 will use when communicating with the TARP router.” (*Id.* at ¶ 0112). Appellant respectfully submits that *Munger*’s hopblocks fail to teach or suggest “an original destination address,” as required by Claim 10.

While *Munger* may discuss the transmission of addresses, *Munger*’s transmitted addresses cannot be characterized as “negotiating translation parameters . . . comprising an original destination address,” since Claim 10 also requires, “changing the packet to have the original destination address, wherein the address change is performed independently from both the first user interface device and the second user interface device.” *Munger* provides no indication that any packet is changed to have the “original destination address,” as required by Claim 1.

Further, *Munger* teaches away from later “changing the packet to have the original destination address,” since *Munger* teaches the use of a different address for the ultimate delivery of a packet. (*Munger* at ¶¶ 0112 & 0115). *Munger* teaches that a router uses the same “IP hopping” to transmit a packet to the final destination. (*Id.* at ¶ 0111). Thus, the destination address would be determined by the hopblock algorithm and would not be the “original destination address” that was a part of the negotiated translation parameters. (*See id.* at ¶ 0109.)

Thus, *Munger* does not describe, expressly or inherently, a method comprising “negotiating translation parameters . . . comprising an original destination address . . .” and “changing the packet to have the original destination address,” as required by Claim 10. Because *Munger* does not disclose, expressly or inherently, every element of independent Claim 10, Appellant respectfully requests reconsideration and allowance of Claim 10 and its respective dependent claims.

III. The proposed *Sheymov-Munger* combination fails to teach or suggest all limitations of Claims 4, 6, 9, 16, 17, 19, 22, 23, 25, and 27 and the proposed combination of *Sheymov* and *Munger* is improper.

The Examiner rejects Claims 4, 6, 9, 16, 17, 19, 22, 23, 25, and 27 under 35 U.S.C. § 103(a) as unpatentable over *Sheymov* in view of *Munger*. To establish a *prima facie* case of obviousness, there must be a suggestion or motivation in the prior art to modify or combine the references, and the combination of reference must teach or suggest all elements of the rejected claims. *In re Vaeck*, 947 F.2d 488, 20 U.S.P.Q.2d 1438 (Fed. Cir. 1991). The Examiner's rejection of Claims 4, 6, 9, 16, 17, 19, 22, 23, 25, and 27 under 35 U.S.C. § 103 fails both of these requirements. First, even if the combination were proper, the proposed *Sheymov-Munger* combination fails to teach or suggest all elements of the claims. Second, there is no suggestion or motivation in the cited references or in the prior art to combine *Sheymov* and *Munger*.

A. *Sheymov* and *Munger*, whether taken alone or in combination, fail to teach or suggest all limitations of dependent Claims 4, 6, 9, 16, 17, 19, 22, 23, and 25 and independent Claim 27.

1. Dependent Claims 4, 6, 9, 16, 17, 19, 22, 23, and 25 are patentable over the *Sheymov-Munger* combination.

As described above, Appellant has shown that *Sheymov* fails to disclose all limitations of independent Claims 1, 14, and 20. Accordingly, *Sheymov* fails to teach or suggest all limitations of Claims 4, 6, 9, 16, 17, 19, 22, 23, and 25 because these dependent claims incorporate the limitations of their respective independent claims. *Munger* fails to remedy the deficiencies of *Sheymov*.

Thus, *Sheymov* and *Munger*, whether taken alone or in combination, fail to teach or suggest all limitations of Claims 4, 6, 9, 16, 17, 19, 22, 23, and 25. Because the references fail to teach all limitations of the claims, Appellant respectfully requests the Board to reverse the Examiner's rejection of Claims 4, 6, 9, 16, 17, 19, 22, 23, and 25 and direct the Examiner to issue a notice of allowance.

2. Independent Claim 27 is patentable over the *Sheymov-Munger* combination.

Consider Claim 27, which recites:

A method for securing packet-based communications comprising:
detecting initiation of a communication stream at a first translation module, the communication stream comprising a plurality of packets from a first user interface device intended for a second user interface device, each packet having an original destination address and an original source address;
identifying a second translation module remote from the first translation module based upon the original destination address;
negotiating translation parameters for the communication stream with the second translation module, the translation parameters comprising an algorithm dictating how to select from among a plurality of modified destination addresses;
receiving the packets; and
for each of the packets, performing an address modification process including selecting one of the modified destination addresses according to the algorithm and changing the original destination address to the selected modified destination address, wherein each of the selected modified destination addresses is resolvable by the second translation module to the original destination address, wherein, except for a first one of the packets, each of the packets is changed to a different one of the modified destination addresses than a preceding one of the packets, and wherein the address modification process is performed independently from both the first user interface device and the second user interface device.

Appellant respectfully submits that *Sheymov* and *Munger*, whether taken alone or in combination, fail to teach or suggest all limitations of this claim, and therefore the Examiner's § 103 rejection based on the *Sheymov-Munger* combination must fail. *See In re Vaeck*, 947 F.2d 488, 20 U.S.P.Q.2d 1438 (Fed. Cir. 1991) (stating that, to establish a *prima facie* case of obviousness, the combination must teach or suggest all elements of the rejected claims).

Among other aspects, *Sheymov* and *Munger* fail to teach or suggest a method "wherein the address modification process is performed independently from both the first user interface device and the second user interface device," as required by Claim 27. As described above, Appellant has shown that *Sheymov* fails to teach or suggest this limitation.

Appellant submits that *Munger* also fails to teach or suggest this limitation. The *Final Office Action* cites *Munger*, page 8, paragraph 0109 as teaching that "the address change is performed independently from both the first user interface device and the second user interface device." (*Final Office Action*, pg. 3). While the router disclosed by *Munger*

“issues separate transmit and receive hopblocks to its clients,” this simply operates to update information stored by the respective clients, similar to the system in *Sheymov*. It is the clients of *Munger* that perform actions. (*Munger* at ¶ 0112 (The router communicates “the transmit and receive hopblocks that the client 801 will use when communicating with the TARP router.”)).

Thus, *Munger* does not teach or suggest, a method “wherein the address modification process is performed independently from both the first user interface device and the second user interface device,” as required by Claim 27. Because *Sheymov* and *Munger*, whether taken alone or in combination, fail to teach or suggest all limitations of Claim 27, Appellant respectfully requests the Board to reverse the Examiner’s rejection of Claim 27 and direct the Examiner to issue a notice of allowance.

B. There is no suggestion or motivation in the cited references or in the prior art to combine *Sheymov* and *Munger*.

The proposed combination of *Sheymov* and *Munger* is improper because the prior art fails to suggest or motivate the proposed combination of the references. The factual inquiry whether to combine references must be thorough and searching. *McGinley v. Franklin Sports, Inc.*, 262 F.3d 1339, 1351-52, 60 U.S.P.Q.2d 1001, 1008 (Fed. Cir. 2001). This factual question cannot be resolved on subjective belief and unknown authority, but must be based on objective evidence of record. See *In re Lee*, 277 F.3d 1338, 1343-44, 61 U.S.P.Q.2d 1430, 1434 (Fed. Cir. 2002).

Nothing in *Sheymov* or *Munger* suggests or motivates the proposed combination. In the *Final Office Action*, the Examiner states:

It would have been obvious to one of ordinary skill in this art at the time the invention was made to combine the teaching of *Sheymov* and *Munger* because they both with [sic] providing network security by varying IP addresses of packets. Furthermore, the teaching of *Munger* to modify the method taught by *Sheymov* to change the source address as well as the destination address would increase security of the traffic in the network by disguising both directions of traffic between nodes (See *Munger*, Paragraphs 0020 and 0021).

Final Office Action, page 8.

Appellant respectfully submits that this statement mischaracterizes the teachings of the references. As discussed in detail above, *Sheymov* fails to teach or suggest changing the

IP address of a packet from an original destination address to a modified destination address. Rather, the alphabetic address known to the user is used to reference the current variable cyber address, which is the only address used in a packet. The variable cyber address, while changing, is not modified once it is included in any given packet. On the other hand, *Munger* varies the IP address of a packet at each hop during transmission of the packet. The cited portion of *Munger* states that address changes can be “done at regular intervals, at random intervals, or upon detection of ‘attacks.’” (*Munger*, ¶ 0020). While *Sheymov* and *Munger* may change addresses at particular times or in response to particular events, these address changes are accomplished in fundamentally different ways.

In short, the motivation provided represents the subjective belief of the Examiner, is not substantiated by any known authority, and therefore is not based on objective evidence of record. Thus, the record fails to provide the required evidence of a teaching, suggestion, or motivation to combine or modify the references, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art.

Appellant thus respectfully requests the Board to find the proposed *Sheymov-Munger* combination improper, reverse the Examiner’s rejection of Claims 4, 6, 9, 16, 17, 19, 22, 23, 25, and 27, and direct the Examiner to issue a notice of allowance.

IV. The proposed *Sheymov-Challenger* combination fails to teach or suggest all limitations of Claim 8.

The Examiner rejects Claim 8 under 35 U.S.C. § 103(a) as unpatentable over *Sheymov* in view of U.S. Published Application No. 2002/10091941 to *Challenger*, et al. (“*Challenger*”). Appellant respectfully submits that *Sheymov* and *Challenger*, whether taken alone or in combination, fail to teach or suggest all limitations of this claim, and therefore the Examiner’s § 103 rejection based on the *Sheymov-Challenger* combination must fail. *See In re Vaeck*, 947 F.2d 488, 20 U.S.P.Q.2d 1438 (Fed. Cir. 1991) (stating that, to establish a *prima facie* case of obviousness, the combination must teach or suggest all elements of the rejected claims).

As described above, Appellant has shown that *Sheymov* fails to disclose all limitations of independent Claim 1. Accordingly, *Sheymov* fails to teach or suggest all limitations of Claims 8 because this dependent claim incorporates the limitations of its respective independent claim. *Challenger* fails to remedy the deficiencies of *Sheymov*.

Thus, *Sheymov* and *Challenger*, whether taken alone or in combination, fail to teach or suggest all limitations of Claim 8. Because the references fail to teach all limitations of the claim, Appellant respectfully requests the Board to reverse the Examiner's rejection of Claim 8 and direct the Examiner to issue a notice of allowance.

Conclusion

Appellant has demonstrated that the present invention, as claimed in Claims 1-27, is patentably distinct from the cited art. Accordingly, Appellant respectfully requests that the Board reverse the final rejection of the Examiner and instruct the Examiner to issue a Notice of Allowance of Claims 1-27.

Appellant encloses a check in the amount of \$500.00 for the filing fee. The Commissioner is hereby authorized to charge any extra fees or credit any overpayments to Deposit Account No. 02-0384 of Baker Botts L.L.P.

Respectfully submitted,

BAKER BOTTS, L.L.P.
Attorneys for Appellant

A handwritten signature in black ink, appearing to read 'K-P', followed by a horizontal line.

Kurt M. Pankratz
Registration No. 46,977
(214) 953-3424

Date: January 30, 2006

Customer No. **05073**

Appendix A: Claims Involved In Appeal

1. (Previously presented) A method for securing packet-based communications comprising:

receiving at a first translation module a stream comprising a plurality of packets regarding a communication from a first user interface device intended for a second user interface device, each packet having an original destination address and an original source address; and

for each of the packets, performing an address modification process including changing the original destination address to a selected one of a plurality of modified destination addresses assigned to a second translation module remote from the first translation module, wherein each of the selected modified destination addresses is resolvable by the second translation module to the original destination address for forwarding the packet to the second user interface device;

wherein the address modification process is performed independently from both the first user interface device and the second user interface device.

2. (Original) The method of Claim 1, wherein, except for a first one of the packets, each of the packets is changed to a different one of the modified destination addresses than a preceding one of the packets.

3. (Original) The method of Claim 1, wherein no more than ten consecutive packets in the stream are changed to an identical one of the modified destination addresses.

4. (Previously presented) The method of Claim 1, further comprising, for each of the packets, changing the original source address to a selected one of a plurality of modified source addresses, wherein each of the selected modified source addresses is resolvable by the second translation module to the original source address.

5. (Previously presented) The method of Claim 1, further comprising randomly selecting the modified destination address for the packet from a range of available destination addresses for the second translation module.

6. (Previously presented) The method of Claim 1, further comprising selecting the modified destination address for the packet from a range of available destination addresses for the second translation module based on a hopping pattern.

7. (Original) The method of Claim 1, wherein the original destination address comprises an internet protocol address and a port, and the modified destination address for the packet comprises a modified internet protocol address and a modified port.

8. (Original) The method of Claim 1, wherein the stream comprises an internet protocol based voice communication session.

9. (Previously presented) The method of Claim 1, further comprising:
detecting initiation of the stream;
identifying the second translation module based upon the original destination address;
and
negotiating translation parameters for the stream with the second translation module,
the translation parameters comprising an algorithm dictating how to select from among the
modified destination addresses.

10. (Previously presented) A method for securing packet-based communications comprising:

negotiating translation parameters with a remote device for a communication stream between a first user interface device and a second user interface device, the translation parameters comprising an original destination address, a plurality of available destination addresses, and an algorithm;

determining a modified destination address from among the available destination addresses according to the algorithm;

receiving a packet of the communication stream having the modified destination address; and

changing the packet to have the original destination address, wherein the address change is performed independently from both the first user interface device and the second user interface device.

11. (Original) The method of Claim 10, wherein:

the translation parameters further comprise an original source address and a plurality of available source addresses; and further comprising:

determining a modified source address from among the available source addresses according to the algorithm.

12. (Original) The method of Claim 11, the packet further having the modified source address, the method further comprising changing the packet to have the original source address.

13. (Original) The method of Claim 10, wherein the algorithm comprises a hopping pattern that dictates how to select from among the available destination addresses.

14. (Previously presented) A first translation module comprising:

a first interface of the first translation module operable to receive a stream comprising a plurality of packets regarding a communication from a first user interface device intended for a second user interface device, each packet having an original destination address and an original source address;

a controller of the first translation module operable, for each of the packets, to perform an address modification process including changing the original destination address to a selected one of a plurality of modified destination addresses assigned to a second translation module remote from the first translation module, wherein each of the selected modified destination addresses is resolvable by the second translation module to the original destination address, wherein the address modification process is performed independently from both the first user interface device and the second user interface device; and

a second interface operable to transmit the changed packets for receipt by the remote device.

15. (Original) The translation module Claim 14, wherein, except for a first one of the packets, each of the packets is changed to a different one of the modified destination addresses than a preceding one of the packets.

16. (Previously presented) The translation module Claim 14, wherein the controller is further operable, for each of the packets, to change the original source address to a selected one of a plurality of modified source addresses, wherein each of the selected modified source addresses is resolvable by the second translation module to the original source address.

17. (Previously presented) The translation module Claim 14, wherein the controller is further operable to select the modified destination address for the packet from a range of available destination addresses for the second translation module based on a hopping pattern.

18. (Original) The translation module Claim 14, wherein the original destination address comprises an internet protocol address and a port, and the modified destination address for the packet comprises a modified internet protocol address and a modified port.

19. (Previously presented) The translation module Claim 14, wherein the controller is further operable to:

detect initiation of the stream;

identify the second translation module based upon the original destination address;

and

negotiate translation parameters for the stream with the second translation module, the translation parameters comprising an algorithm dictating how to select from among the modified destination addresses.

20. (Previously presented) Logic for securing packet-based communications, the logic encoded in a medium and operable when executed to:

receive at a first translation module a stream comprising a plurality of packets regarding a communication from a first user interface device intended for a second user interface device, each packet having an original destination address and an original source address; and

for each of the packets, perform an address modification process including changing the original destination address to a selected one of a plurality of modified destination addresses assigned to a second translation module remote from the first translation module, wherein each of the selected modified destination addresses is resolvable by the second translation module to the original destination address, wherein the address modification process is performed independently from both the first user interface device and the second user interface device.

21. (Original) The logic of Claim 20, wherein, except for a first one of the packets, each of the packets is changed to a different one of the modified destination addresses than a preceding one of the packets.

22. (Previously presented) The logic of Claim 20, further operable, for each of the packets, to change the original source address to a selected one of a plurality of modified source addresses, wherein each of the selected modified source addresses is resolvable by the second translation module to the original source address.

23. (Previously presented) The logic of Claim 20, further operable to select the modified destination address for the packet from a range of available destination addresses for the second translation module based on a hopping pattern.

24. (Original) The logic of Claim 20, wherein the original destination address comprises an internet protocol address and a port, and the modified destination address for the packet comprises a modified internet protocol address and a modified port.

25. (Previously presented) The logic of Claim 20, further operable to:
detect initiation of the stream;
identify the second translation module based upon the original destination address;
and
negotiate translation parameters for the stream with the second translation module, the translation parameters comprising an algorithm dictating how to select from among the modified destination addresses.

26. (Previously presented) A first translation module comprising:

means for receiving at the first translation module a stream comprising a plurality of packets regarding a communication from a first user interface device intended for a second user interface device, each packet having an original destination address and an original source address; and

means for performing at the first translation module an address modification process including, for each of the packets, changing the original destination address to a selected one of a plurality of modified destination addresses assigned to a second translation module remote from the first translation module, wherein each of the selected modified destination addresses is resolvable by the second translation module to the original destination address for forwarding the packet to the second user interface device;

wherein the address modification process is performed independently from both the first user interface device and the second user interface device.

27. (Previously presented) A method for securing packet-based communications comprising:

detecting initiation of a communication stream at a first translation module, the communication stream comprising a plurality of packets from a first user interface device intended for a second user interface device, each packet having an original destination address and an original source address;

identifying a second translation module remote from the first translation module based upon the original destination address;

negotiating translation parameters for the communication stream with the second translation module, the translation parameters comprising an algorithm dictating how to select from among a plurality of modified destination addresses;

receiving the packets; and

for each of the packets, performing an address modification process including selecting one of the modified destination addresses according to the algorithm and changing the original destination address to the selected modified destination address, wherein each of the selected modified destination addresses is resolvable by the second translation module to the original destination address, wherein, except for a first one of the packets, each of the packets is changed to a different one of the modified destination addresses than a preceding one of the packets, and wherein the address modification process is performed independently from both the first user interface device and the second user interface device.

Appendix B: Evidence

NONE

Appendix C: Related Proceedings

NONE



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: McDaniel, David W.
Serial No.: 10/072,069
Filing Date: February 05, 2002
Confirmation No. 1183
Group Art Unit: 2154
Examiner: Ashokkumar B. Patel
Title: Address Hopping of Packet-Based Communications

Mail Stop Appeal Brief - Patents
Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Dear Sir:

CERTIFICATE OF MAILING BY EXPRESS MAIL

I hereby certify that the attached Appeal Brief (34 pages), check in the amount of \$500.00, Baker Botts return postcard (1 postcard), and this Certificate of Mailing are being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 C.F.R. § 1.10 on this 30th of January 2006 and is addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Willie Jiles

Willie Jiles

Express Mail Receipt
No. EV 732498966 US